Republic of Namibia

Ministry of Information & Communication Technology

Namibia

National Cybersecurity Strategy & Awareness Raising Plan **2022 - 2027**

"A step towards Cyber resilience & Digital Security"





TABLE OF CONTENTS

Acknowledgements iv
Foreword v
Acronyms and abbreviations vi
PART ONE: National Cybersecurity Strategy 1
1. Introduction 2
2. Background 3
3. Methodology 5
4. Current Situation: 6
5. Digital Landscape 7
6. High-level statements 8
6.1. Vision 8
6.2. Mission 8
6.3. Strategic Goals 8
6.4. The Guiding Principles. 9
7. National Cybersecurity Strategy Framework 10
8. Strategic Pillars 11
9. SWOT ANALYSIS 14
9.1. National Cyber Security Strategy: Strengths 14
9.2. National Cyber Security Strategy: Weaknesses 15
9.3. National Cyber Security Strategy: Opportunities 15
9.4. National Cyber Security Strategy: Threats 15
10. Cyber Threats and Attack Vectors 16
11. Risks and Mitigation Strategies 17
PART TWO - Cybersecurity Awareness raising campaign 22
1. Introduction 24
2. Objectives 25
3. Campaign focus 25
4. SWOT ANALYSIS 27
a. Strengths 27
b. Weaknesses 27
c. Opportunities 28
d. Threats 28
5. Target Audience 29
6. Key Messages 31

7. Strategies 31
8. Communication Channels 31
9. Review and evaluation / impact assessment 32
References 33

APPENDIX

APPENDIX 1: Notional Implementation Plan and Costs 34
APPENDIX 2: Monitoring and Evaluation 37

ACKNOWLEDGEMENTS

The Government of the Republic of Namibia hereby expresses its sincere gratitude and appreciation to the Commonwealth Secretariat for its assistance; for their contributions and support; distinguished appreciation goes to the following institutions: Office of the Prime Minister; Office of the President; Ministry of Home Affairs, Immigration, Safety & Security; Namibia University of Science & Technology, and Internet Society Namibia Chapter for availing staff members who voluntarily took time out of their busy schedules to participate in finalizing the drafting and completion of this national document.

FOREWORD



Namibia strives to be among the leading nations in adopting and using the latest technologies like Digital TV, 4G, and the West Africa Cable System (WACS) to name a few and efforts are underway to diversify and stimulate a greater growth in the sector to improve the level of access to basic communication and broadband usage, and services.

With our focus on realizing a prosperous and industrialised Namibia, developed by her human resources, enjoying peace, harmony and political stability. A successful realization of our Vision 2030 depends highly on our ability to safeguard our cyberspace, data, technologies, Critical National Infrastructure (CNI), and Critical National Information Infrastructure (CNII) from the cyber security threats that are becoming more sophisticated and resulting in financial losses and related risks. Recently, Namibia has encountered rise in incidents of misuse of available internet platforms/ networks by criminals to carry out cyber-attacks, this can happen anytime, against anyone, and from anywhere. The growing cyber threats disturb the purposes of digital participation and connectivity as well as the integrity of our nation's critical infrastructure.

More Namibians are becoming more connected and depend on networks for information and communication, business transactions and trading. Cabinet has taken decisive action to protect its economy and netizens' privacy by approving the development of the National Cyber Security Strategy and Awareness Raising Plan. The strategy aims to outline modalities to safeguard the netizen's privacy, educate and create awareness, information, sharing and collaboration on cyber security.

The implementation of this Strategy is through a multi-stakeholders' approach and it can only be through togetherness that we will prosper.

DR. PEYA MUSHELENGA, MP

MINISTER OF ICT

ACRONYMS AND ABBREVIATIONS

Acronyms and abbreviations

CIs	Critical Infrastructures
CNI	Critical National Infrastructure
CNII	Critical National Information Infrastructure
CRAN	Communications Regulatory Authority of Namibia
DDoS	Distributed Denial of Service Attack
GFCE	Global Forum for Cybersecurity Expertise
ICT	Information and Communication Technology
ISO	International Standards Organization
KPIs	Key Performance Indicators
MICT	Ministry of Information and Communication Technology
NCIRT	National Cybersecurity Incident Response Team
NIPAM	Namibia Institute for Public Administration and Management
PPP	Public/Private Partnership
SADC	Southern Africa Development Community
SWOT	Strengths, Weaknesses, Opportunities, and Threats
UN	United Nations
WACS	West Africa Cable System
4G	Fourth Generation



PART ONE:
National Cybersecurity Strategy

1. INTRODUCTION

In Namibia telecommunication services increased rapidly when mobiles services were introduced in 1995. This has led Namibia to participate in the undersea cable project by joining other African Countries and inaugurating the 14,000 km West Africa Cable System (WACS) from London to the Swakopmund Landing Station in 2012. The WACS submarine cable was constructed to meet the local increasing internet bandwidth demand.

As Namibians are becoming more connected and become more reliant on information and communication to capitalize on the benefits and opportunities accorded by ICTs every day, there is a growing misuse of cyberspace and networks by criminals that disturb the purposes of digital participation and connectivity as well as the integrity of the nation's critical infrastructure. Small economies like Namibia are becoming more targeted and inclined to the cyber threats because of the absence of a national Cyber Security Strategy and Awareness Plan and an incidence response body to monitor, detect threats and respond quickly as well as to collect and store data on cyber incidences.

In March 2020, Kaspersky.com ranked Namibia at 119 globally as being subjected to cyber-attacks. The following are some of the cyber-attacks that affected Namibia in the past; crypto miners, mobile cyber-attacks and ransomware attacks. The economic sectors such as education, government and communications were listed as the most common targets in Namibia.

Recognising the significance of ICT usage and the need to effectively and collectively respond to cyber threats, Cabinet has approved the development of the National Cyber Security Strategy and Awareness Raising Plan which aims to safeguard the National Critical Information Infrastructure, educate and create awareness, information sharing and collaboration on cyber security and continuously improve the safety of vulnerable groups in the cyberspace.

Namibia National Cybersecurity Strategy &Awareness Raising Plan is a six-year living document (2022 – 2027) which is a step towards Cyber resilience & Digital Security to enable an innovative Namibia and achievement of social and economic growth. Through ensuring that the nation responds effectively to threats on network systems/ services and recovers from them.

2. BACKGROUND

The Government of Namibia has articulated through its Vision 2030 plan its intent to develop 'A prosperous and industrialised Namibia developed by her human resources, enjoying peace, harmony and political stability'. Linked to this Vision is the Ministry of ICT Strategic Plan 2017-2022, which specifies its mission as 'To create an enabling environment for ICT development and access to information for socio-economic growth'.

These two documents indicate the importance of technology in achieving the nation's ambitious development objectives. Significant advances within the penetration of technology are already underway with mobile subscribers exceeding 2.7 million, internet usage reaching 96 percent of the population, 3G broadband access available to 75 percent of the population, and 4G to 48 percent 26 multipurpose community centers have been opened in remote areas of the country.

The growing scourge of cybercrime has the potential to negatively impact the nation's ability to achieve its development objectives. Technology platforms need to be protected and the most vulnerable need to be aware of and educated regarding the perils of the Internet. Because of the complexity of cybercrime and cybersecurity, Namibia approached the Commonwealth Secretariat and Council of Europe to assist with the refinement of the Cybercrime and Data Protection Bill. A joint in-country mission of the aforementioned institutions plus the World Bank and the United Kingdom Foreign Commonwealth Office was undertaken in May 2019 to conduct a needs assessment to review the Cybercrime Bill and other relevant legislation and conduct a review of the Cybersecurity landscape to identify gaps and potential vulnerabilities and assess the level of Cybersecurity maturity in Namibia. The May 2019 mission identified a series of gaps and vulnerabilities:

- The current Cybercrime Bill is not aligned with the Budapest Convention which is internationally recognised as the leading treaty on cybercrime legislation. The Government of Namibia has indicated their desire to accede to the Convention.
- A National Cybersecurity Strategy has not been developed to coordinate and focus technology investments to improve the security of technology platforms.
- There is a lack of awareness and urgency to address the growing threats of cyber-attacks and an understanding of the significant social and economic impacts of a successful attack.

- There is an acute shortage of skilled and experienced cyber personnel to implement and maintain security policies and procedures.
- A National Cybersecurity Incident Response Team is not in place. Such a team is critical in managing cyber events and bringing back into operation affected systems in an expeditious manner.

As a result of the May 2019 mission findings, the Commonwealth Secretariat and the Council of Europe returned in February 2020 to address the following high priority next steps:

- Conduct a detailed analysis of the Cybercrime Bill using the Budapest Convention as the target legislation and identify areas that require modification.
- Review options for a Data Protection Bill, and provide recommendations to align the bill with international legal conventions.
- Draft a National Cybersecurity Strategy that is based on input from a wide variety of stakeholders. This 'Made in Namibia' strategy is critical to secure ownership, buy-in, and commitment, especially from senior executives in Government and the private sector.
- Draft a National Cybersecurity Awareness plan to inform and educate all sectors of Namibian society on the dangers of the internet and safe practices to utilise when accessing the internet.

The Commonwealth Secretariat together with the Ministry of ICT held a consultative workshop which was attended by participants from multiple sectors, including government, banking, telecommunications operators, the telecommunications regulator, academia, legal, computer software and equipment businesses, and Parliamentarians. The workshop participants provided inputs that resulted in a draft National Cybersecurity and draft National Cybersecurity Awareness Raising Plan. To that effect, the Ministry of ICT approached Cabinet for approval to develop the said Strategy, approval was granted and a multi-stakeholders Committee was established under the chairmanship of MICT.

The Committee commenced work on a 2 years term appointment to finalize the Strategy and its awareness-raising Plan. The Committee made use of the source documents and models developed by the Commonwealth Secretariat or in collaboration with other international organizations which guided the discussions during the workshop and preparation of this report. Those models included the following: The International Telecommunications Union Guide; the Commonwealth Cybercrime Initiative Assessment Checklist; and the Organization of American States guide to developing a Cybersecurity Awareness Raising program. Others included the Commonwealth Secretariat/Council of Europe assessment report of May 2019 (Namibia), the World Bank/Oxford Maturity Assessment report; reports from global cybersecurity organizations to identify best practices in cybersecurity

awareness-raising programs; and other guiding principles are sourced from national documents such as Namibia Vision 2030, the draft Cybercrime Bill (2019), Data Protection Bill (2013), and the Overarching ICT policy (2009).

3. METHODOLOGY

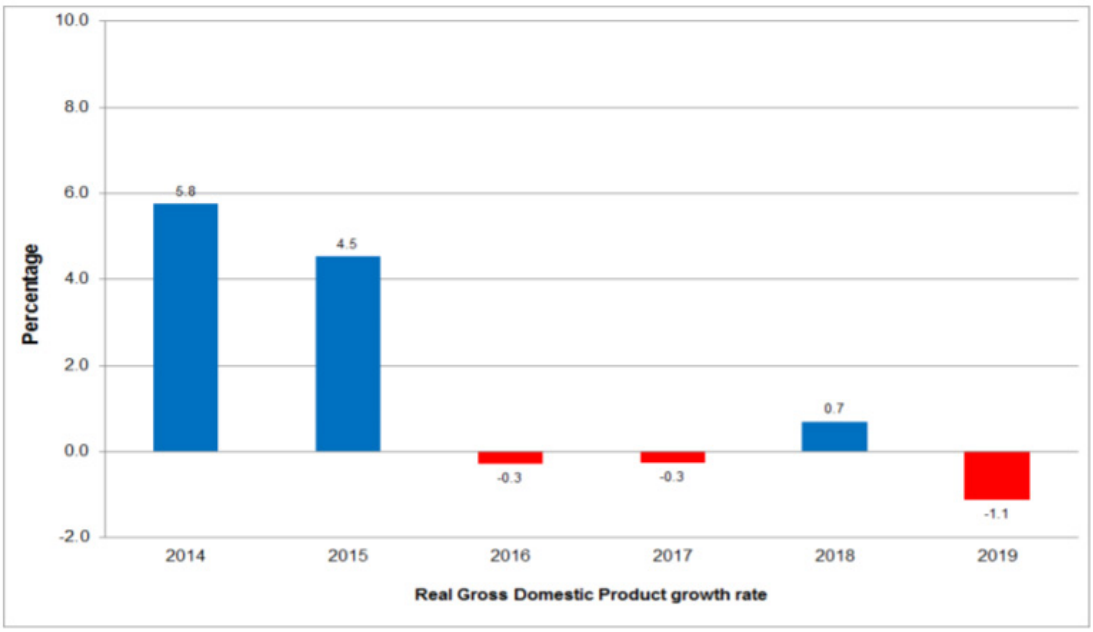
The methodology to develop this document included the following:

- Review of the Cybersecurity landscape to identify gaps and potential vulnerabilities and assess the level of Cybersecurity maturity in Namibia;
- Stakeholders workshop to provide the inputs which resulted in the draft;
- Preparation of draft documents and circulation to stakeholders for comments;
- Cabinet approval to develop the Strategy and Plan;
- Composition of the Committee to drive the finalization of the Strategy and Plan;
- Circulation of the draft to stakeholders for comments;
- Preparation of the draft Strategy and Plan;
- Stakeholders' validation Workshop;
- Processing of the Strategy and Plan for approval and adoption.

4. ECONOMIC OVERVIEW OF THE ICT INDUSTRY

Namibia is classified as an upper middle-economy in Africa by the World Bank. It is estimated that the GDP per capita was US$ 5,028 in 2019. The table below shows that the economy has been contracting since 2016 and continued to be weak in 2019 contracting by 1.1 percent compared to a slightly positive performance of 0.7 percent in 2018.

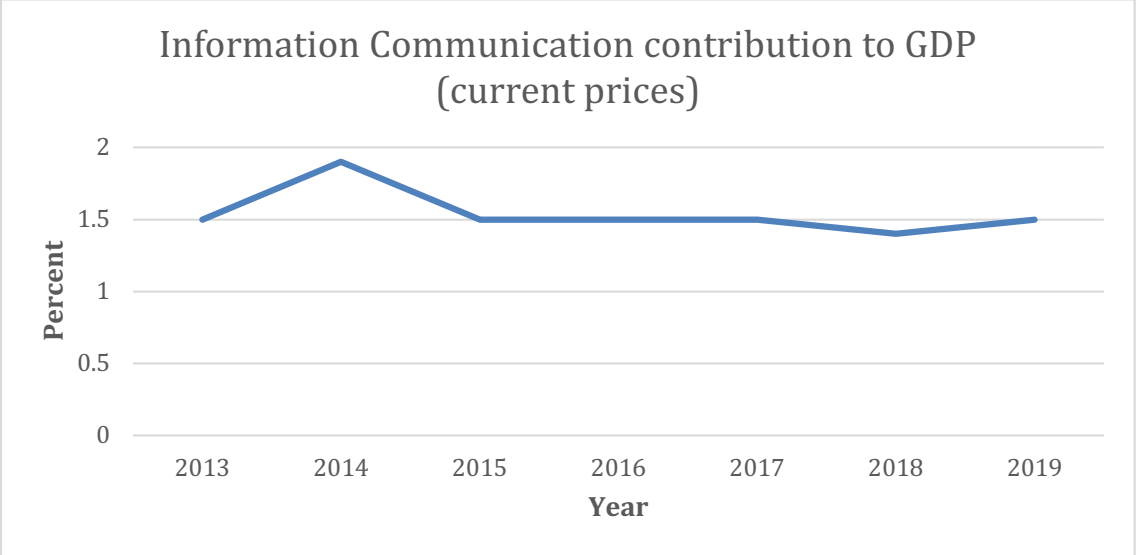
Figure 1: ***GDP Growth Rate 2014-2019***



Source: NSA-2018

As much as Information and Communication Technologies (ICTs) can accelerate and transform enterprises and government, as well as, stimulate entrepreneurship, innovation and economic growth, their contribution to the GDP is fairly constant, this is depicted in the table below. Information Communication contributed a mere 1.4% to GDP in 2019.

Figure 2: ICT contribution to GDP at current prices



3. Employment Level in ICTs and Wages

ICT employment is defined as the people working in the Information and Communication sector. As per the 2018 Namibian Labor Force Survey employment in the sector increased by 20% from 5,973 employees in 2016 to 7,141 employees in 2018.

The highest average wage was earned by a person working in the financial and insurance industry at N$ 20,459 per month. On average a person working in the Information and Communication sector is paid N$17,139, this is the fourth-highest paying sector in Namibia. There is still a gap between the salaries of men and women (Gender wage gap) in the sector as on average, a man is paid N$ 17,192 compared to N$ 16,967 paid to a woman.

5. DIGITAL LANDSCAPE

The Ministry of ICT developed a 2017 – 2022 Strategic Plan which provides a roadmap to achieve its vision of 'A catalyst for an informed and inclusive ICT smart Namibia'. The Plan is linked to the following national and international development agendas: Namibia Vision 2030; the Southern Africa Development Community (SADC) Vision; and the African Union Vision. These linkages demonstrate how technology will contribute to these agendas and provide a basis for securing funding to implement the final cybersecurity strategy. Since it is recognized that technology is a key enabler to implement the Namibia Vision 2030, funding for this initiative must include a technology component.

The United Nations (UN) conducts an e-Government survey2 every two years to assess the e-Readiness of 194 countries and one of the variables for the assessment is the maturity of telecommunications infrastructure. The variable includes the percentage of the population

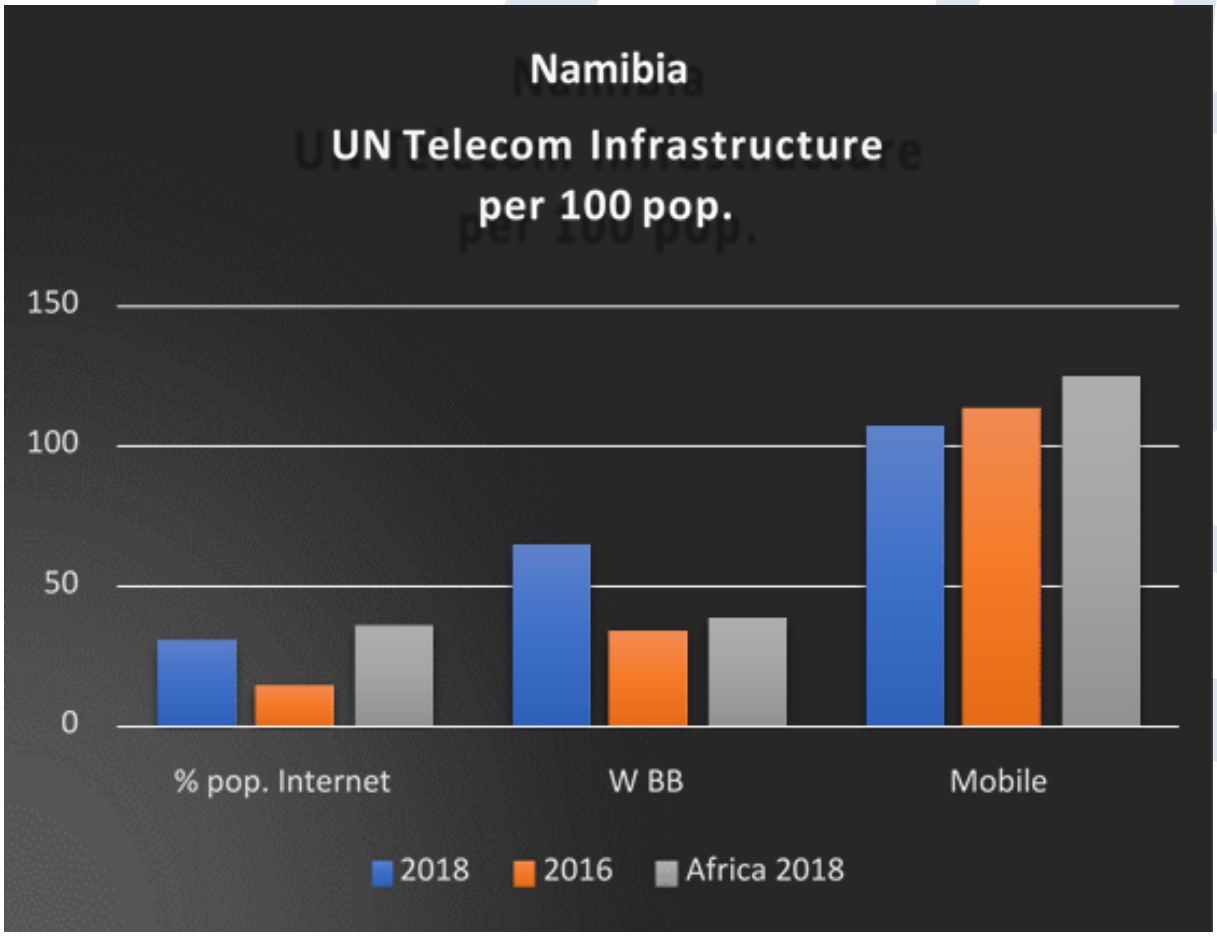
using the internet, the percentage of the population with wireless broadband, and the penetration rate for mobile devices.

Figure 3: Provides further details from the survey on Namibia's telecommunications infrastructure. Some notable statistics: Penetration rates for mobile devices exceeded 100 percent, which may be due to the affordability of these devices and access to mobile services; Wireless broadband (high-speed internet) penetration has increased over 90 percent from 2016 (32.4 percent of the population) to 2018 (64.9 percent of the population).

The competitive mobile rates may have contributed to this increase. Wireless broadband penetration in Namibia (65 percent of the population) is above the average across Sub-Sahara Africa (39 percent of the population); Number of users on the internet has increased from 2016 (14.84 percent of the population) to 2018 (31.03 percent population). The Communications Regulatory Authority of Namibia (CRAN) expects that the number of internet users will increase to 96.4 percent of the population in 2020.

The developments indicated by these statistics amplify the critical need to improve cybersecurity policies and procedures. Without a robust program to protect technology platforms, hackers can exploit vulnerabilities to obtain sensitive personal and financial information. This can lead to cost increases for delivering services, elevating reputational risk and jeopardizing the successful implementation of national social and economic development agendas.

Figure 3: Telecom Infrastructure per 100 pop **Source: UN Report**



6. HIGH-LEVEL STATEMENTS

6.1. Vision

A secured cyberspace to enable an innovative Namibia and achievement of social and economic growth

6.2. Mission

Establish resilient infrastructure, legislation, and increase cybersecurity capabilities in Namibia.

6.3. Strategic Goals

1. The overall goal is to establish a resilient infrastructure – improve the detection, analysis, mitigation and response to cyber threats, critical infrastructure and other systems of national interest.

2. Legislation's enforcement - maintain an effective legal framework and enforcement capabilities to target and prosecute cyber-crime, and

3. Increase Cybersecurity Capabilities - promote the development of a skilled cyber security workforce with access to research and development for innovative solutions in Namibia.

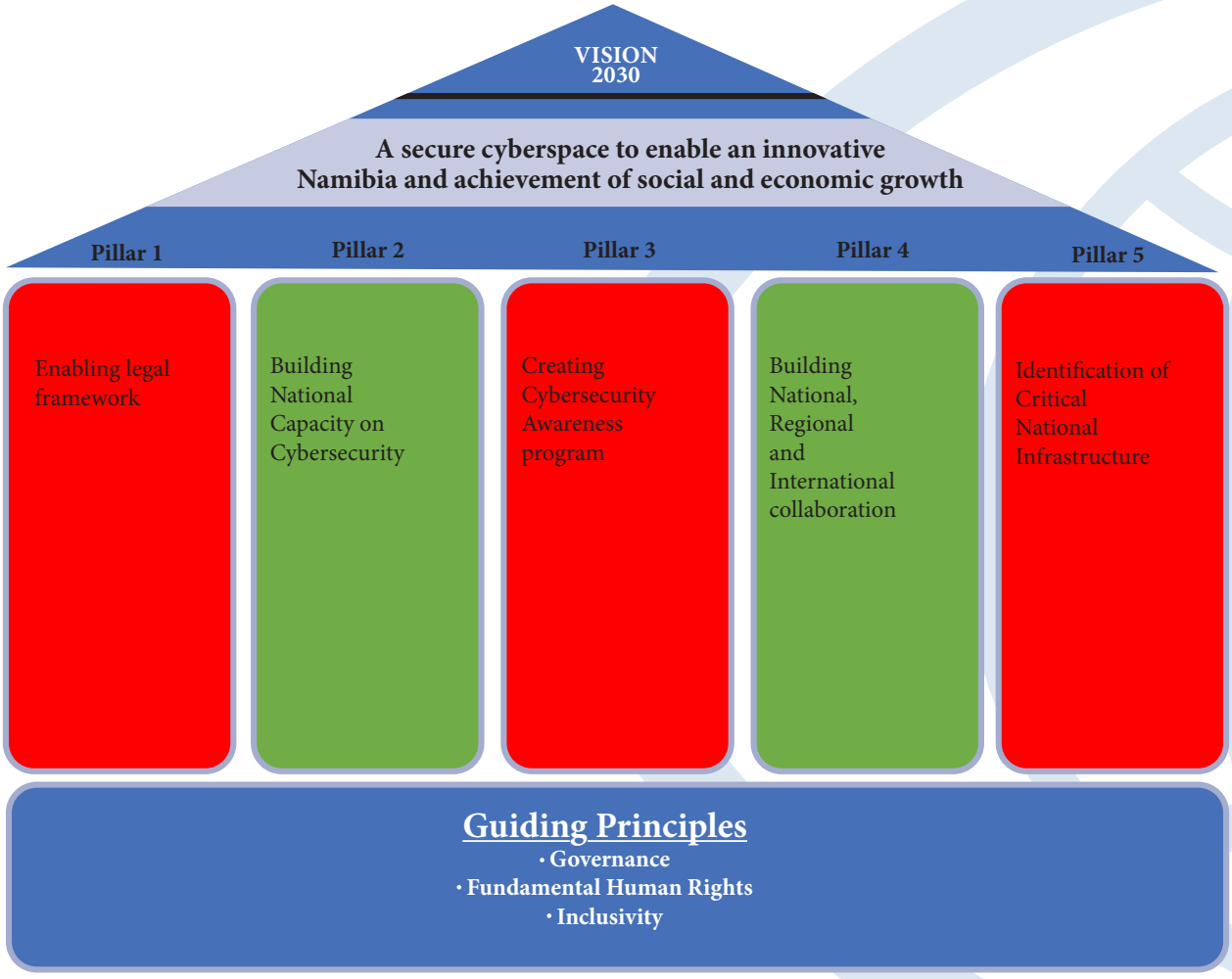
6.4. The Guiding Principles.

These cross-cutting issues/guiding principles were considered when designing the Strategy:

- Governance - the Strategy should identify and empower the competent authority accountable for the execution of the Strategy; establish a mechanism to identify and include the government entities affected by, or responsible for, the implementation of the Strategy; commit to including specific, measurable, attainable, result-based and time-based objectives in the implementation plan for the Strategy.
- Fundamental Human Rights - it should respect universally agreed fundamental rights, including, but not limited to, the United Nations' Universal Declaration of Human Rights and International Covenant on Civil and Political Rights, as well as relevant multilateral or regional legal frameworks. Attention should be paid to freedom of expression, the privacy of communications and personal data protection.
- Inclusivity - identifying and engaging all the relevant stakeholders is essential to the

development and successful implementation of a National Cybersecurity Strategy. This will help understand stakeholder needs and their unique knowledge and expertise, thus facilitating cooperation towards achieving the objectives of the Strategy. Special attention should be focused on persons with special needs to ensure that design parameters take into consideration these requirements.

In addition to the four components, risk and mitigation strategies and a national implementation plan with estimated costs are included to emphasize the importance of commitment and the magnitude of the effort required to implement the Strategy.



7. STRATEGIC PILLARS

As indicated above, the strategic pillars are the initiatives that will enable the achievement of the National Cybersecurity Vision and are the considered opinions of the participants in the February 2020 Windhoek workshop. Each pillar is discussed in detail below and should be viewed in a national context. Recommendations for the Government of Namibia are included for each pillar and contain the key deliverables required to achieve the objectives for the pillar.

Pillar 1: Enabling legal framework

The objective of this pillar is to prioritize & fast-tracking the adoption of modern and robust cybercrime legislation, in line with international standards, which could allow to effectively tackle the challenges currently faced in cyberspace. Suitable legal provisions are needed to facilitate the cross-country investigation, prosecution and adjudication of cyber and cyber-related crimes.

Strategic objective 1: Develop and/or review the necessary legislation, policies, and regulations

Strategies

1. Finalize Draft Data Protection Bill
2. Finalize the Draft Cybercrime Bill

Pillar 2: Building National Capacity on Cybersecurity

The objectives for this pillar are: to create a National Cybersecurity Incident Response Team (NCIRT) to manage cyber events and be the focal point to coordinate incident reports, communicate to key stakeholders and devise cyber policies and procedures; and develop a national pool of skilled and experienced security personnel to address the growing need for this type of expertise. Further, this strategic pillar seeks to strengthen the capacity to prevent and respond to malicious cyber activities.

Strategic Objective 2:

1. To have recognized and functional National Cybersecurity structures

Strategies

1. Establish a National Cybersecurity Incident Response Team for Namibia
2. Develop and implement Cyber Hygiene Policies and campaigns to mitigates over 80 percent of all cyber threats
3. Promote and support the development of cybersecurity curricula to address market demand

Pillar 3: Creating Cybersecurity Awareness program

The objectives for this pillar are: to elevate the level of national awareness of the perils of the internet and steps to utilize the internet safely; and to educate senior executives in government and the private sector on the devastating impact of a successful attack and secure their commitment to treating this issue as a national priority. Further, the pillar seeks to educate all netizens (internet users) on the internet benefits and dangers in order to practice safe habits to avoid harm or compromise their privacy while surfing cyberspace.

Strategic objective 3: Create and promote awareness among internet users and promote cyber hygiene.

Strategies

1. Develop a national cybersecurity awareness-raising plan/program;
2. Develop and publish awareness creation materials;
3. Conduct targeted awareness creation campaigns nationwide on multiple platforms.

Pillar 4: Building National, Regional and International collaboration

The Government of the reoublic of Namibia, in close collaboration with stakeholders, and the private sector will take the leadership role to advance cybersecurity in Namibia. The Government will demonstrate leadership in advancing Namibia's cyber security interests both locally and abroad, by ensuring the enhanced collaboration and coordination of strategic cyber security and cybercrime issues amongst stakeholders, and by advocating for an open, free and secure internet. The objectives for this pillar are: to increase the level of national and international collaboration; and to adopt, where applicable, international cybersecurity standards, policies and treaties.

Strategic Objective 4:

- Establish and coordinate national, sub-regional, continental, and international collaborations on cybersecurity
- Define cyber defense, mitigation, and incident response strategies for government and non-governmental institutions, as well as netizens;

Strategies

1. Create a Public/Private Partnership (PPP) and cooperations in efforts to curb cybercrimes/offenses;
2. Accede to the international treaties and mutual assistance conventions;
3. Ministry of ICT to serve as the focal point for national and international cybersecurity cooperation for sharing of intelligence, training staff and supporting cyber events.
4. Adhere to International Standards such as International Standards Organization (e.g. ISO 27001)
5. Develop information-sharing mechanisms on cyber threats and attacks amongst the public and private sectors.

Pillar 5: Identification of Critical National Infrastructure

The Critical National Infrastructure (CNIs) are regarded as those critical elements of infrastructure such as assets, facilities, systems, networks, or processes and workers that operates and facilitates these infrastructures. The objectives for this pillar are: to create a comprehensive list of CNIs and periodically update the list to maintain its currency; and to conduct a risk assessment and use the results to prioritize investments in high-risk areas.

CNIs are information and communication assets that perform vital functions which are important to the proper operation of social and economic activities.

Strategic objective 5: Safeguard Critical National Infrastructure (CNIs) and Critical National Information Infrastructure (CNIIs)

Strategies

1. Create a list of CNI & CNII Assets list – the initial steps taken by the Multi-Sectorial Steering Committee should be continued and signed off by Government and CNI organizations. CRAN should coordinate the efforts to establish the CNIs list and ensure that it is periodically updated.
2. Conduct a risk assessment to prioritize investments in high-risk areas – there are limited resources available to address cybersecurity threats and funding should be directed towards high-risk challenges with a particular focus on CNIs. Conduct the risk assessment exercises.
3. Create a CNI secure community to share information and collaborate in addressing cyber events – the Ministry of ICT should initiate and lead the development

of this community. Key actions for the community to consider are: develop a clear governance framework where roles and responsibilities for community members should be clearly defined and mechanisms to encourage compliance with community standards; report cyber events immediately to alert community members to potential threats and to take all necessary precautions; collaborate and support members in addressing cyber events through the deployment of skilled resources; share best practices and lessons learned, and create a base level of cybersecurity standards for CNIs – the standards could adhere to international practices such as the National Institute of Standards and Technology -

https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

8. SWOT ANALYSIS

8.1. National Cyber Security Strategy: Strengths

- The Government of the Republic Namibia has drafted relevant Bills which are yet to be enacted. These Bills ensure that the legal framework is sufficient in addressing various vectors of the threats that consumers may experience in cyberspace. It also allows the National Cybersecurity Strategy and Awareness Raising Plan to be developed with established legal support.
- The drafted relevant Bills allow the National Cybersecurity Strategy and Awareness Raising Plan to be developed with established legal support.
- The existing close collaboration between Government and stakeholders, territories and the private sector plays a role to advance cybersecurity in Namibia
- The offering of IT and cybersecurity-related courses and programs at the local universities and cum availability of experts and graduates in the said fields to assist in safekeeping cyberspace and protect the national critical assets.
- By establishing the National Cybersecurity Strategy and Awareness Raising Plan, Namibian businesses would experience a boom in digital innovations, and as a result, the nation would see an increment in business investment as well as growth in digital markets.

The strategy will create a framework for a national CERT/CSIRT which would then serve as a platform where law enforcers and government officials can join hands to share information on mitigating cyber threats.

8.2. National Cyber Security Strategy: Weaknesses

- Though relevant Bills have been drafted, there are no laws at the moment to ensure confidence and security in/of online transactions and services; and for the protection of vulnerable members of the Namibia society such as children.
- Limited funding from the government and other leading institutions to accelerate cyber security initiatives.
- The progress of the cyber security strategy implementation is dependent on relevant legal instruments which are still in the draft phase.

8.3. National Cyber Security Strategy: Opportunities

- There is an increased interest in cyber security studies amongst tertiary students, which has the potential to increase the cyber security skills gap in Namibia.
- Namibia could experience a boom in the number of cyber security experts and professionals, which could potentially allow the cyber security community to thrive and innovate more advanced countermeasures against the evolving threats, which could effectively allow us to prevent and/or mitigate any wide-scale cyber-attacks that may seek to exploit vulnerabilities.
- The move will nurture the cyber security ecosystem of Namibia by allowing more digital security startups to take the stage and present innovative products and services that are built to reinforce online security.

8.4. National Cyber Security Strategy: Threats

- Implementation might be a bit slow due to the absence of adequate legislation, shortage of resources, and skilled hands while security threats are continually evolving.
- There is no recognized platform for entities (public and private) to share information regarding data breach incidents.
- Entities are unwilling to share data breach incidents with others out of fear of victimization and reputation risks.

9. CYBER THREATS AND ATTACK VECTORS

A cyber threat can be defined as any malicious act mounted against a digital device, that has the potential to violate any of the principles of the Central Intelligence Agency (CIA) triad, using the cyber-space. Namibia has witnessed an increase in internet coverage, internet speed, and an increase in usage of internet-enabled devices in the past couple of years, which has improved information sharing. These advances in technology have revolutionized the digital landscape in Namibia and have proved to benefit our communities in terms of service delivery. Indeed, the potential for digital transformation to deliver new business value is huge, but so is the potential for redefined security risks.

Symantec, together with the African Union Commission, published a report under the Global Forum for Cybersecurity Expertise (GFCE) detailing cybersecurity trends in Africa from the continental perspective. The 3 major cyber threats facing this region included:

- Smartphones and the Internet of Things – with the high penetration rate of mobile devices in Kenya, the increase of mobile malware, especially with Apple IOS software, will continue with a focus on M-Pesa (mobile banking) transactions;
- Crypto ransomware insertions were identified as another attack vector that will continue to disrupt the operations of businesses, government and banking institutions. The new cryptography algorithms will become more difficult to decode, forcing the victims to pay the ransom demanded.
- Social engineering, a psychological technique used by hackers to trick victims into providing sensitive information, via email scams is the most common method to insert malicious codes into technology platforms, resulting in compromised systems.

Deloitte conducted a Cyber Security Survey4 for Namibia that included senior technology officers in both private and public sector organisations. The purpose of the report was to use the survey data to assist Namibian organisations to manage and respond to cyber risk, potential cyber security attacks, as well as the impact this has on the company. The report indicated that the types of cyber incidents experienced included: Hacking, Malware, Ransomware and Social Engineering.

Kaspersky, a leading Cybersecurity company, indicated in their November 2015 report on online threats suggested that Namibia was ranked fourth in malware banking attacks among all countries that utilised Kaspersky products. 5 2.9 percent of these attacks were directed toward Namibia.

Two major cyber events were reported in Namibia during 2018 - 2019. Namely a Ransomware attack and Distributed Denial of Service Attack (DDoS). During the May 2019 workshop meetings participants mentioned, several other cyber-attacks were not reported due to reputational risk and embarrassment.

10. RISKS AND MITIGATION STRATEGIES

The table below lists the risks that were identified by the participants in the February 2020 workshop while the mitigation strategies, probabilities, and impact were based on the experiences of the Commonwealth Secretariat's consultant. It should also be noted that the risks were not categorized by Pillar since each risk could apply to several pillars.

Rating: **1 – low to 5 – high (See Table Next page)#**	**Risk**	**Mitigation** **Strategy**	**Prob.**	**Impact**	**Risk Factor**
	INTERNAL				
1	**Lack of political support/ commitment** • Resistance to change by politicians • Lack of accountability • Change in political leadership	The benefits of robust cybersecurity and the devastating consequences of a successful attack should be clearly delineated. The impact on citizens and possible impact on political electability could also be mentioned.	5	5	25
2	**Inadequate resources (funding, staff, infrastructure)** • High costs to implement Strategy • Other high priority projects may compete for resources	Raise the level of cybercrime awareness with a focus on senior executives to secure funding. Engage regional and international bodies to provide funding and funding in kind. Establish Public Private .	5	5	25

3	**Obsolete technology platforms and infrastructure** • Technical risks due to lack of skilled staff and outdated infrastructure • Underestimating the complexities and challenges associated with this initiative	Engage the Namibia University of Science and Technology to build capacity. Utilize the perspective 'think big, start small and scale fast' to breakdown complex initiatives into manageable deliverables. Work with developed countries to facilitate skills exchange programs.	4	4	16
4	**Delays in promulgation of Laws and Regulations** • Implementation of Strategy could be affected due to delays in passing relevant laws e.g. cybercrime bill • Legislation / Strategy cannot keep pace with the fast pace of technological change	Design and development of initiatives could be conducted in parallel to legislative approval. Increase the level of cybercrime awareness with Parliamentarians to convey the importance and urgency to pass Cybercrime laws. Avoid using specific technologies in Legislations Review and Revise the legislation/ strategy to keep up with technologies change.	4 5	3 5	12 25

5	**Lack of Mandatory Registration of Prepaid SIM Card Users** • Social engineering and SIM boxing will tread in • Mobile commerce (m-Commerce) opportunities created • The greater consumer will freely access to e-Government services	Recommends policy-makers to /by: Operationalise Part 6 of Chapter V of the Communication Act. Engaging and consulting with local mobile operators who are best placed to suggest implementation methods. Conducting a full impact assessment of the proposed policy including its costs and benefits; Taking into account global best practices and insights; and Ensuring that their proposed rules are proportionate and relevant to the specific market.	5	5	25
6.	**Absence/Inadequate continuity of operations and disaster recovery plans**	Develop a national standard plant/system disaster recovery plans and ensure every institution has a plan in place that an associated with cyber contingency plan and cyber security incident response plan	5	5	25

7	**Inadequate periodic security audits**	Develop national guidelines for periodic security audits that focus on assessing security controls at the various levels, such as people and policy, operational, network, platform, application, process, physical security, and third-party relationships	5	5	25
8	**Insufficient identity validation and background checks on the new hires**	Institute appropriate procedures to conduct background checks of all new hires. Further, prior to being granted access to sensitive information and resources, proper authentication and authorization mechanisms are required	5	5	25
9.	**Absence of an institutional security awareness program**	Every institution should have a security awareness program to ensure that all personnel have an understanding of sensitive information, common security risks, and basic steps to prevent security breaches	5	5	25
10.	**Absence of the National Computer Incidence Response Team (CIRT) in Namibia**	Establish a National Cybersecurity Incident Response Team in Namibia.	5	5	25
11.	**Lack of awareness on the seriousness and impact of cyber-attack among the community**	Create community awareness on cyber attack	4	3	12

External					
#	**Risk**	**The Mitigation Strategy**	**Prob.**	**Impact**	**Risk Factor**
1	**Reputational risk** • Loss of confidence by external investors in the security of technology platforms • Lack of consumer confidence, trust to purchase/ trade goods online • Decline in global financial ratings / rankings • Changes/advancements in technology infrastructure and systems	Key factor is to implement at least Basic Cyber hygiene practices which could mitigate over 80 percent of cyber threats. Adopt international standards, where appropriate, to add another layer of credibility. Develop an effective awareness raising program to educate investors steps being taken to improve cybersecurity practices.	3	3	9
	The increased pace of cyber-attacks by external parties • Kaspersky – 2.9 percent of Banking Trojans directed to Namibia banks • Critical infrastructure will continue to be vulnerable	Implement at a minimum basic Cyber Hygiene practices. Provide a standard set of cybersecurity policies and practices for Critical Infrastructure.	4	4	16
2	**Cannot align with international laws, conventions and treaties** • International standards require modern and secure technological platforms	Request the owners of these conventions and treaties to provide funding and funding in kind to support the implementation of these agreements.	3	2	6

PART TWO
Cybersecurity Awareness Raising Plan

1. INTRODUCTION

Namibia is one of the frontrunners in Africa on ICT development, with internet access well established, wide coverage connectivity and fairly stable speed. In the past two years' internet penetration in the country stood at 52% with 1.28 million internet users, 710000 thousand social media users and a total of 76,000 online shoppers. The said statistics manifest that Namibians are progressivley getting connected to the Internet and the use of ICTs is definitely booming ultimately today than ever. It is however with great distress that this increased connectivity and growing dependence on the use of ICTs poses extreme vulnerability, disturbances and increased threats to the economic activities of people, the functionality of business, networks, and the critical national infrastructures.

It is against the above that Namibia realized that the nation will only reap the spillover benefits and economic opportunities presented by the use of ICTs on the condition that the country is ready, capable, and vigilant against the threats that include phishing attacks, ransomware, cyberbullying, and child online vulnerability. Hence, it is in this cognizance that the government identified National Cybersecurity Awareness as one of the mechanisms to respond effectively to cyber threats by developing an implementable Cybersecurity Awareness Plan. Changing behavior requires more than providing information about risks and reactive behaviors – firstly, people must be able to understand and apply the advice, and secondly, they must be motivated and willing to do so – and the latter requires changes to attitudes and intentions.

The campaign focuses on public messages to promote responsible usage of the Internet and create awareness of fraud, identity theft, cyber predators, and cyber ethics. Apart from cybersecurity awareness campaigns using different platforms, all Offices, Ministries, Agencies, and Organizations (OMAs) should conduct cybersecurity awareness presentations to all employee, to sensitize members on cyberspace threats.

This campaign is aimed at bringing the message on cybersecurity to deliver the following outputs:

- Increased knowledge about Cybersecurity amid growing threats and attacks;
- Safeguard the netizens and the national critical infrastructures
- Fostered behaviors changes to reduce Cybersecurity;
- Encouraged sympathy and support towards Cyber-attack/threat victims;
- Internet users are safer and more secure online.
- Increased preparedness and managed disturbances caused by cyber threats

2. OBJECTIVES

Together with its stakeholders and interested partners, the Ministry of Information and Communication Technology members will pursue opportunities for collaboration on raising cybersecurity awareness in all institutions within the borders of this land of the brave. Our collaborative efforts aim to achieve the following:

- Create and promote awareness among internet users and promote cyber hygiene.
- Engages citizens (of all age groups), reduce risk and ultimately helps create a culture of Cyber cautious
- Educate citizens on the importance of cybersecurity and personal data protection
- Engage and secure senior executives to promote and support cybersecurity initiatives

3. CAMPAIGN FOCUS

In our attempts to increase public awareness about cybersecurity, ultimately increasing the understanding of cyber threats and empowering the public to be prepared and secure. Before getting into the discussions on the targeted focus areas, it is worth narrating in brief the top cybersecurity threats to be aware of during the COVID -19 pandemic and beyond.

3.1. Phishing Attacks

It is the most common type of cyberattack that aims to steal sensitive data like credit card or debit card numbers and login information. Since the advent of the Corona Virus pandemic, Cybercriminals are taking advantage of the pandemic by sending fraudulent emails and WhatsApp messages that attempt to deceive you into opening attachments or clicking on malicious links to have important updates or encouraging donations impersonating trustworthy organizations.

3.2. Ransomware Attacks

The COVID-19 pandemic has set stress on healthcare systems and public institutions around the world. More patients and distracted employees are being targeted by cybercriminals for ransomware attacks since they cannot afford to be logged out of their systems due to the current health crisis. Cybercriminals believe they are likely to pay the ransom. Hence, targeted ransomware has become one of the biggest cybersecurity threats of 2020 and beyond.

3.3. End-point security threats

With COVID-19 infections on the rise, many Government institutions and private businesses were compelled to go fully remote, and “the work-from-home” became the new norm. Remote workers often work devoid of any network security, thus missing out on a crucial part of layered cybersecurity protection. In addition to this, mobile devices can often end up masking signs indicative of potential phishing attacks and other cybersecurity threats.

3.4. Malware

Cybercriminals are exploiting the widespread global communications on the COVID-19 to mask their activities. Malware, spyware and Trojans have been found embedded in interactive applications, social media links and websites. Spam emails are also deceiving users into clicking on links that download malware to their devices.

3.5. Insiders/employees as Threats

Insider threats not only include malicious attacks, but also the negligent use of systems and data by employees. To safeguard against these threats, it is essential that organizations quickly and accurately detect, inspect, and respond to issues that could be indicators of insider attacks. Common antivirus and anti-malware tools are generally ineffective against these threats. Insider threats require specialized tools that may merge machine learning and intelligent tagging to detect unusual activity, suspicious changes, and threats caused by system misconfigurations.

3.6. Unpatched Vulnerabilities Open Doors for Hackers

Programs that haven't been updated often serve as open doors for cyber-attackers looking to launch malware in unpatched, or unknown, vulnerabilities. An example last year (2020) hackers were able to use the Blue-Keep exploit to hack into unpatched Windows systems to install a cryptocurrency miner. The good news is that these highly destructive threats are also some of the easiest to prevent with good patch management practices. It is now so evident that cybersecurity is one of the biggest threats to the global economy, so it's no secret that cybersecurity will represent one of the biggest challenges for Governments and enterprise organizations over the next decade.

Our approach to raising awareness of cyber-related threats, empowering and educate government officials, the private sector and individuals with the much-needed knowledge to combat the ever-evolving cyber-related threats or issues and share responsibilities, practice safe and informed behaviors on the Internet will focus on the following:

- Fraud & Phishing – to educate users of possible forms of fraud and phishing activities they are likely to fall prey to.
- Ransomware & Malware attacks – to sensitize users on the strategies used by cybercriminals to penetrate their networks, spread the malware/ransomware that will have a disruptive effect on the network and cause malfunctioning of systems, applications and hardware. Sometimes the restoration is made tougher because of the denial of services effect.
- Child online – to educate parents, guardians and children on the dangers of being online and sensitize them on ethical and safe usage of the internet.
- Privacy and Data protection – to educate the corporate and individual citizens on matters related to privacy and personal/institutional data protection strategies.

❖ Collaboration & information exchange – to create awareness of available modalities for crisis communications and collaboration in fighting cybercrimes.

4. STRENGTHS, WEAKNESSES, OPPORTUNITIES, AND THREATS (SWOT) ANALYSIS

The 4th Strategic Pillar under the title Cybersecurity Awareness seeks to educate all netizens (internet users) on the benefits of using the internet and the dangers associated with it. The objective of this pillar is to promote cyber hygiene by creating awareness among internet users. The SWOT analysis discussed in this section presents the Strengths, Weaknesses, Opportunities, and Threats of the strategies that seek to aid the pillar in achieving its strategic objective.

a. Strengths

- The wide coverage of mobile networks in Namibia allows for wider outreach of audiences should mobile platforms be used for awareness. According to TheGlobalEconomy.com, by 2016 Namibia has achieved 100% mobile network coverage, which is calculated based on the percentage of the population. https://www.theglobaleconomy.com/Namibia/Mobile_network_coverage/
- Social Media – most of internet users are on Social Media, which is available at no cost.
- Radio – is available almost everywhere in Namibia.
- TV – Namibia has a national, community and commercial broadcasters that can be used to help in cyber awareness.
- Email – most companies and government institutions have private email addresses that can be used to share information on cybersecurity awareness.
- Government educational institution is another strength that can be utilized e.g. Cyber security awareness can easily incorporate as part of the syllabus.

b. Weaknesses

- Awareness programs could require funding, for which at this point there has not been an indication for funding from the ministry.
- Cyber security awareness is a project that involves funds that in most cases the government does not have.
- The cyber-security Committee does not have the necessary expertise to design sophisticated cybersecurity posters and flyers.
- Most remote areas still do not have internet, or radio services available so it is difficult for

people in remote areas to access awareness programs.

- Most people have very little to no computer literacy so it is difficult for them to understand basic cyber-security.
- Technology is forever evolving so today's awareness might not be relevant tomorrow.

c. Opportunities

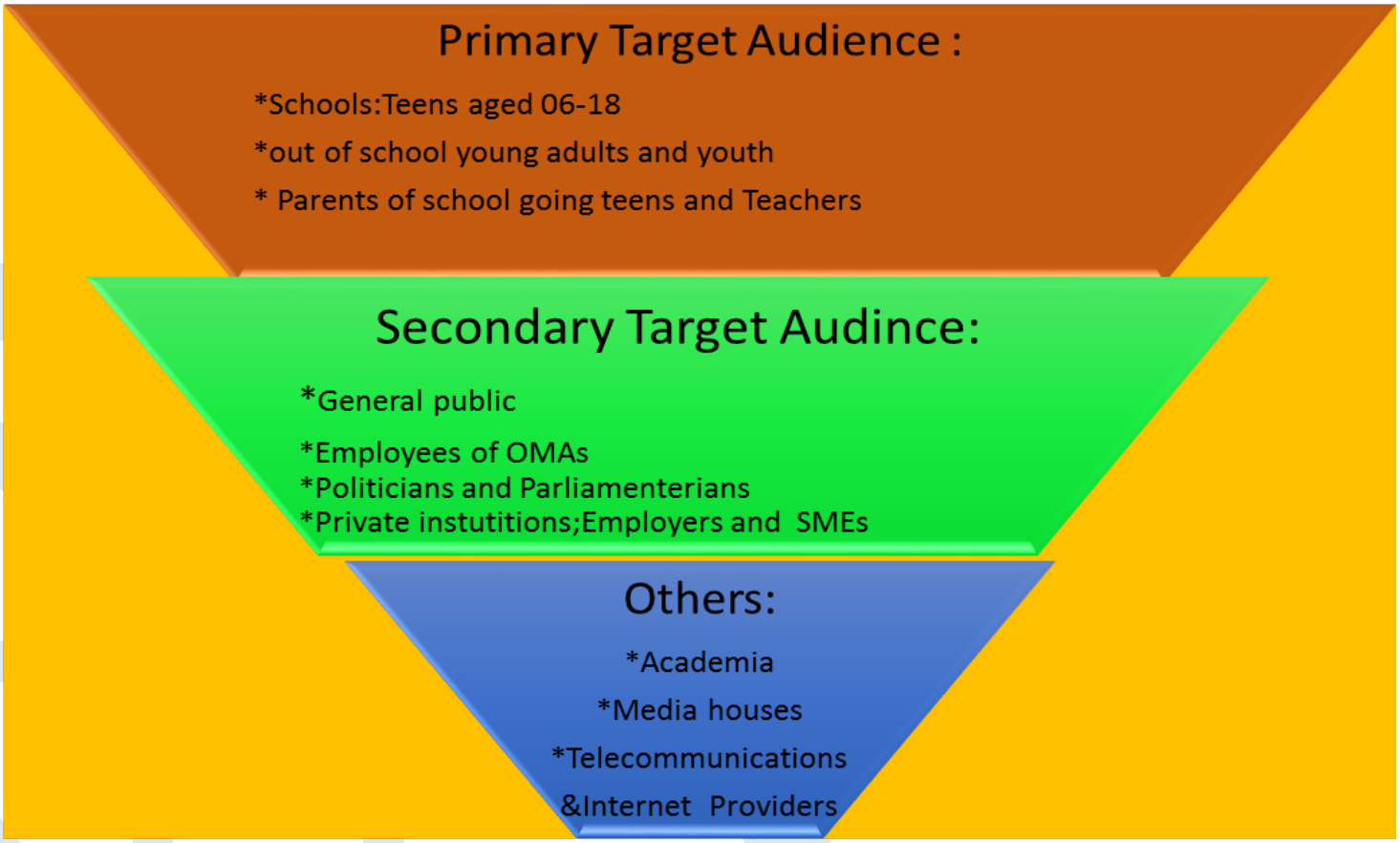
- The Ministry enjoys good relationships which various companies, who may be willing to assist and contribute to the awareness programs.
- According to Statista a German company specializing in market and consumer data the number of mobile cellular subscriptions per 100 inhabitants in Namibia has significantly increased between 2000 and 2019. Which presents an opportunity to take advantage of mobile platforms to reach a good number of users. https://www.statista.com/statistics/509593/mobile-cellular-subscriptions-per-100-inhabitants-in-namibia/
- There are institutions like Namibia Institute for Public Administration and Management (NIPAM) that can be used to educate the user in government and other institutions at no extra cost.
- Most private institutions will be willing to assist the government in cyber-security awareness.
- Most Social Media Platforms can be used at no extra cost; this is a great opportunity because most internet users are on Social Media.
- Radio broadcast in Namibia is the media with the most audients almost every household in Namibia has access to a radio.

d. Threats

- The rolling out of the awareness programs could be costly.
- The COVID-19 regulations might limit strategies and ideas on how awareness programs could be carried out.
- Hackers who are highly skilled will have access to cyber security awareness information, which they could use to re-adjust and advance their skills. They could also use similar adverts for phishing.

5. TARGET AUDIENCE

National Cybersecurity Awareness Target Audience



s/no	Target Audience	Motivational Reasons
01	**Parents and General Public**	The first step in educating children about cyber-security starts with training parents in this area. Children's access to technology comes with additional responsibility for the parents. Beyond the dangers children can face in the online environment, parents need to be aware of the fact that the inattention with which they provide access to the child's technology can have consequences that go beyond family boundaries.

02	**Children**	Nowadays children are using the internet on a daily basis for many reasons; playing online games, social media or even for doing their school works. The internet takes a huge part of their time and unfortunately, most of these children are not aware of online risks and how they should respond properly to online risks. Moreover, children may have unlimited access to the internet without any control or supervision. The cyber-crimes are increasing year after a year and the Namibian government should consider the safety of the citizens as one of the priorities to achieve
03	**Employees and Employers**	It has also been well documented that employee negligence has been responsible for some of the worst cyber breaches in history. It has been reported that 90% of all cyber-attacks are caused by human error. Such statistics highlight the prevalence of security threats that organizations face and the need to ensure Cyber Security awareness at all levels. The key to an effective security awareness program is ensuring the right training is targeted at the right people. All users are susceptible to cyber threats; however, certain employees have a higher threat profile than others. Therefore, a Cybersecurity awareness campaign should start with HR and Finance Departments in all ministries. These departments will be frequently targeted because of their privileged access to sensitive data.

6. KEY MESSAGES

The Namibian Government recognizes that effective, integrated and coordinated communication is integral to carrying out National Cyber Security Strategy and Awareness's goal to build a better, digitalized future for people all over the country. The purpose of this Framework is to describe a strategic approach for effectively communicating National Cyber Security Strategy and Awareness information, advice and guidance across a broad range of cyber security issues: from data privacy issues to emerging and novel risks. Key messages will be framed around the following:

- Cybersecurity for safer internet usage in Namibia
- Cyber hygiene & ethics
- Cybersecurity, rules and standards for personal safety & privacy
- Phishing – typical messages, forms, strategies, and risks
- Malware

7. STRATEGIES

Dependent upon the communication channel used, regular reminders/marketing information should be sent out on various communication channels including paid advertisements on various media platforms. Advances in technology have created additional avenues to deliver and/or receive information. Considering the number of potential audience tools available today, a campaign with the right marketing mix can be very effective. For instance, this campaign should include the following elements:

- **Media Relations** – Develop awareness messages to be released targeting Editors and Reporters to reach audiences through media.
- **Community Relations** – Develop "direct-connect" opportunities to reach audiences that are considered as stakeholders, for example, parents, children, employees, employers, and various community groups.
- **Website enhancement** – existing ministerial website to be enhanced with relevant content and key messages with the aim to deliver the information to the target audience.
- **Advertising** – Create effective, key message-based advertisements for print, TV, radio, online media and posters.

8. COMMUNICATION CHANNELS

Effective mapping of communications channels will ensure National Cyber Security Strategy's messages are disseminated through multiple channels so that audiences receive National Cyber Security Strategy information, advice, and guidance several times from a range of sources.

Communication channels tend to fall into four main categories.

- **Mass Media -** These channels have a broad reach and include television, radio, newspapers, magazines, outdoor and transit advertising, direct mail, and websites. Mass media channels, such as radio, community billboards, and posters on public transportation, have broad reach and can increase issue awareness. Placement through these channels may be free or may incur a cost if placement on certain platforms or at specific times is important.
- **Social Media -** platforms touch millions of followers, including Twitter, Facebook, and WhatsApp.
- **Organization and community** - These channels reach specific groups of individuals based on geography (for example, a specific village) or a common interest, such as occupational status. Channels may include community-based media, such as local radio talk shows, organization newsletters; community-based activities, such as meetings at schools, workplaces, and houses of worship.
- **Interpersonal** - People seeking advice or sharing information about cybersecurity risks often turn to family, friends, consumer groups, and partner organisations. These one-on-one discussions are often the most trusted channels for cybersecurity information. Interpersonal channels are especially important when trying to influence attitudes and encourage wider adoption of cybersecurity behaviors.

Factors to consider when prioritizing channels include their reach (number of people that will hear, see, or read a message), and how the channel supports audiences' ability to recall the message and impact (whether the message results in action). Exposure to the message and repetition are key to audience recall, increasing the likelihood that audiences will act on the information provided.

9. REVIEW AND EVALUATION/IMPACT ASSESSMENT

Periodic reviews and evaluations of programs and plans are critical to assess whether the campaign is still relevant in light of the changing risk environment and whether it still reflects the objectives and what adjustments are needed to make it a better fit and relevant. In addition, regular reviews and monitoring are aimed at assessing the progress made with regards to the objective, it is important to periodically evaluate the outcomes and map them back to the objectives set. The monitoring evaluation will be coordinated by the Ministry of ICT in corroboration with National Planning Commission as well as other stakeholders. Based on the outcomes of the evaluation, a review of the awareness plan will be recommended on the merits of the gaps identified and recommendations provided.

REFERENCES

1. Proxima Networks (2021), https://www.proximanetworks.com/blog/top-5-cybersecurity-threats-in-times-of-covid-19/,
2. National Cybersecurity Strategy Good Practice – ITU and Commonwealth Secretariat. See Overarching Principles page 30
3. CNBC (2019), Cybersecurity is the biggest threat to the world economy over the next decade, CEOs say: https://www.cnbc.com/2019/07/09/cybersecurity-biggest-threat-to-world-economy-ceos-say.html , Accessed: 8 June 2021.
4. ZDNet (2019), BlueKeep attacks are happening, but it's not a worm, https://www.zdnet.com/article/bluekeep-attacks-are-happening-but-its-not-a-worm/, Accessed: 8 June 2021.
5. The GlobalEconomy.com (2021), Namibia: Mobile network coverage: https://www.theglobaleconomy.com/Namibia/Mobile_network_coverage/ , Accessed: 8 June 2021.

APPENDIX 1: NATIONAL IMPLEMENTATION PLAN AND COSTS

The table below summarizes the Key Performance Indicators (KPIs) for each action, the targets, estimated costs, roles and responsibilities of stakeholders.

Pillar	Action(s)	KPI	Base line	Time frame and targets per year						Budget Estimate (NAD),000					Respon-si ble/ Lead entity
				21/22	22/23	23/24	24/25	25/26	26/27	21/ 22	22/ 23	23/ 24	24/ 25	25/ 26	
Enabling legal framework	Finalize data protec-tion bill.	% of progress made on the Promulgation of Data Pro-tection Bill	98%	98.5%	100%	-	-	-	-	150	200	-	-	-	-MICT -MoJ-(CCL) -Attorney General Office -Cabinet -National Assembly -National Council
	Finalize Cyber-crime law.	% of progress made on the enactment of the Cybercrime law	96%	97%	98%	100%				20	500	500			-MICT -MoJ-(CCL) -Cabinet -Na-tional Assem-bly -Na-tional Coun-cil
Building National Capacity on Cyberse-curity	Establish a NCSIRT	% of Progress made on the establishment of NCSIRT			10%	50%	100%								-CRAN -OPM -MICT

Promote the develop-ment/ implemen-tation of cyber hygiene policies/ proce dures	# of engagement sessions held on institutional cyber hygiene policies/ procedures	0	-	2	3	4	4	4	-	30	30	30	30	MICT

	Increase expertise in the area of cybersecurity	Number of cybersecurity expertise produced		21	20		35	35	35						UNAM, NUST
Creating Cybersecurity Awareness program	Develop a Cybersecurity program	% of progress made on the development of a Cybersecurity awareness program	0	100%						-	-	-	-	-	-MICT
		Number of awareness sessions held	1	20	10	10	10	10	10	100	100	100	100	100	MICT & Salt Essentials Namibia
		Number of awareness materials produced	0	2	4	4	4	4	4						MICT Salt Essentials Namibia OMAs
Building National, Regional and International collaboration	MoU signed on cybersecurity	Number of MoU signed on cybersecurity	0	1											MICT
	Establish PPPs	# of PPP signed	0		1	1	1	1	1	100	100	100	100	100	MICT and stakeholders

APPENDIX 2: MONITORING AND EVALUATION

The strategy presented as a five-year roadmap to achieve the set targets whilst prioritizing the budget and setting timelines with responsible parties or entities for each activity. The Implementation Action Strategy sets performance and verifiable targets and allocates responsibilities for implementation to different institutions that include Government and other key stakeholders. Continuous monitoring of the implementation of the targets in the strategy is a critical commitment whereas, the evaluation will assess the impact of the progress towards attainment of the set targets periodically. It is recommendable that the evaluation is conducted by an independent external evaluator at the end of the strategy implementation time frame.

Strategic Pillar	Project/ Activities	KPI	Target	Actual(achievement)	Key challenges	Recommendations for improvement/way forward	Reporting institution
Enabling legal framework	Finalize data protection bill.	% of progress made on the Promulgation of Data					
	Finalize Cybercrime laws.	% of progress made on Cybercrime lawenacted					
Building National Capacity on Cybersecurity	Establish a NCSIRT	% of Progress made on the establishment of NCSIRT					
	Establish PPPs	# of PPP signed					
	Develop & implement cyber hygiene policies/campaigns	# of Security, policies and procedures developed					
	Promote & support the development of cybersecurity curricula	Number of cybersecurity programmes implemented at universities/colleges					

Creating Cybersecurity Awareness program	• Develop a Cybersecurity Awareness Raising Plan	% of progress made on the development of a National cybersecurity awareness-raising plan/strategy Number of awareness sessions held					
		Number of awareness materials produced					
Building National, Regional & International collaboration	MoU signed on Cybersecurity	Number of MoU signed on Cybersecurity					

Identification of Critical National Infrastructure	Develop an official register of National Critical Infrastructures (CIs)	An official register of National CriticalInfrastructures (CIs) produced					

